CLAIMS

1. A method of managing an hierarchy of nodes manipulated by processing apparatus, the method comprising a step of permitting access to a particular node of the hierarchy only after receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes.

2. A method according to claim 1, wherein said step is carried out in a tamper-resistant hardware module.

3. A method according to claim 1, wherein said mechanism is a protected process executing in a benign operating environment within the apparatus, the method further comprising using a trusted source to establish or initiate establishment of said mechanism and to generate said reliable indication accordingly.

4. A method according to claim 3, wherein each non-leaf node of said hierarchy comprises a key used to encrypt the or each of its child nodes, said particular node being a node, below the top level of the hierarchy, that comprises a particular key associated with said protected process, this key being made available for use in relation to the protected process upon said reliable indication being received.

5. A method according to claim 4, wherein said particular key forms the root of an hierarchy of cryptographically-protected objects associated with the protected process.

6. A method according to claim 4, wherein said step is carried out in a tamper-resistant hardware module separate from said trusted source.

7. A method according to claim 6, wherein said particular key forms the root of an hierarchy of cryptographically-protected objects associated with the protected process.

8. A method according to claim 6, wherein said particular key is made available by revealing it unencrypted outside of said module to the protected process, the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendant nodes, being carried out by said protected process outside of said module.

9. A method according to claim 6, wherein the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendant nodes, are carried out within said module, the module responding to the trusted source providing said reliable indication in respect of said protected process to internally store a release indicator in respect of said particular node, descendants of said particular node being tagged with an identifier of said particular node, and the module only permitting access to a said descendant of said particular node when the identifier associated with the node concerned corresponds to a stored release indicator.

10. A method according to claim 6, wherein making said particular key available comprises installing it as the current operative root node of said tree-structure hierarchy such that those parts of the hierarchy that can only be reached by ascent from the current root node are inaccessible, the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendent nodes, being carried out within said module.

11. A method according to claim 3, wherein access to said particular node is further conditional upon presentation of an authorisation.

12. A method according to claim 11, wherein said authorisation is a digest of the protected process, the trusted source calculating this digest from the protected process code to be executed.

13. A method according to claim 3, wherein said trusted source is a hardware root of trust.

14. A method according to claim 3, wherein said trusted source is a protected compartment operating system executing on the apparatus.

15. A method according to claim 6, wherein the tamper-resistant module holds, in unencrypted form the top-level node of said hierarchy, the other nodes of the hierarchy being stored in encrypted form separately from the key-handling unit when not being used.

16. A method according to claim 6, wherein the tamper-resistant module is a Trusted Platform Module according to the TCPA architecture.

17. Processing apparatus for managing an hierarchy of nodes, the apparatus comprising an access-control arrangement for permitting access to a particular node of the hierarchy only upon receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes.

18. Apparatus according to claim 17, wherein the access-control arrangement is implemented in a tamper-resistant hardware module.

19. Apparatus according to claim 17, further comprising means for implementing said mechanism as a protected process executing in a benign operating environment within the apparatus, and a trusted source for initiating said mechanism and generating said reliable indication accordingly.

20. Apparatus according to claim 19, wherein the access control arrangement is provided by a key-handling unit and each non-leaf node of said hierarchy comprises a key used to encrypt the or each of its child nodes, said particular node being a node below the top level of the hierarchy that comprises a particular key associated with said protected process, the key-handling unit being arranged to make this key available for use in relation to the protected process upon said reliable indication being received.

21. Apparatus according to claim 20, wherein said particular key is arranged to form the root of an hierarchy of cryptographically-protected objects associated with the protected process.

22. Apparatus according to claim 20, wherein the key-handling unit takes the form of a tamper-resistant hardware module separate from said trusted source.

23. Apparatus according to claim 22, wherein said particular key is arranged to form the root of an hierarchy of cryptographically-protected objects associated with the protected process.

24. Apparatus according to claim 22, wherein the key-handling means is arranged to make said particular key available by releasing it unencrypted to the protected process; the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendent nodes, being arranged to be carried out by said protected process when executing in the apparatus.

25. Apparatus according to claim 22, wherein the key-handling unit comprises:

- first means responsive to the trusted source providing said reliable indication in respect of said protected process to store a release indicator in respect of said particular node;
- second means for permitting access, within the key-handling unit, to a node only when the node concerned has an identifier indicating a relationship with a node for which a said release indicator has been stored by the first means;
- third means for carrying out cryptographic use of said particular key and cryptographic operations for accessing any of its descendent nodes.

26. Apparatus according to claim 22, wherein the key-handling means is arranged to make said particular key available by installing it as the current operative root node of said tree-structure hierarchy handled by the key-handling unit such that those parts of the hierarchy that can only be reached by ascent from the current root node are inaccessible, the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendent nodes, being arranged to be carried out by the key-handling unit.

27. Apparatus according to claim 19, wherein the access-control arrangement is arranged such that access to said particular node is further conditional upon presentation of an authorisation to the access-control arrangement.

28. Apparatus according to claim 27, wherein said authorisation is a digest of the protected process, the trusted source being arranged to calculate this digest from the protected process code to be executed.

29. Apparatus according to claim 19, wherein said trusted source is a hardware root of trust.

30. Apparatus according to claim 19, wherein said trusted source is a protected compartment operating system arranged to execute on the apparatus.

31. Apparatus according to claim 22, wherein the key-handling unit is arranged to hold, in unencrypted form the top-level node of said hierarchy, the key-handling unit being further arranged to store the other nodes of the hierarchy in encrypted form separately from the key-handling unit.

32. Apparatus according to claim 22, wherein the key-handling unit is a Trusted Platform Module according to the TCPA architecture.

33. Processing apparatus comprising a key-handling unit for handling a tree-structured hierarchy in which each non-leaf node comprises a key used to encrypt the or each of its child nodes, the hierarchy including, below its top level, a node comprising a particular key associated with a protected process executable by the processing apparatus; the key-handling unit being arranged to make said particular key available for use in relation to the protected process upon receipt both of authorisation to do so and an indication that the authorisation is provided by a trusted source that is arranged to provide this authorisation, and to initiate or permit execution of said protected process, only after verifying the presence of a benign operating environment within the apparatus for said protected process.

34. Apparatus according to claim 33, further comprising said trusted source.

35. Apparatus comprising a key-handling unit for handling a tree-structured key hierarchy, the key-handling unit being arranged to treat a selected node of the hierarchy as the current root node such that those parts of the hierarchy that can only be reached by ascent from the current root node are inaccessible, the key-handling unit including an arrangement for changing the node of the hierarchy serving as said current root node.

36. Apparatus according to claim 35, wherein the arrangement for changing the current root node is enabled to do so only upon a predetermined set of at least one condition being met.

37. Apparatus according to claim 36, wherein at least one predetermined condition comprises the receipt of an authorisation value indicative of digital data.

38. Apparatus according to claim 37, wherein said authorisation value is a digest of a protected process associated with the node that is intended to be the new current root node

39. Apparatus according to claim 36, wherein at least one predetermined condition comprises that a protected process associated with the node that is intended to be the new current root node is about to be run by the apparatus.

40. Apparatus according to claim 39, wherein at least one predetermined condition comprises that any other currently-activated processes running on the apparatus are benign.

41. Apparatus according to claim 36, wherein at least one predetermined condition comprises that the key-handling apparatus is requested to change the current root node by a root of trust of the apparatus.

42. Apparatus according to claim 35, wherein the node at the head of the hierarchy as judged without regard to which node is the current root node, forms said current root node upon start of the apparatus.

43. Apparatus according to claim 35, wherein the key-handling unit is arranged to hold the current root node internally in unencrypted form at least whilst it remains the current root node.

44. Apparatus according to claim 35, wherein the key-handling unit is arranged always to hold the node at the head of the hierarchy, as judged without regard to which node is the current root node, internally in unencrypted form.

45. Apparatus according to claim 35, wherein the key-handling unit is a Trusted Platform Module according to the TCPA architecture.

46. Apparatus according to claim 35, wherein the key-handling unit is arranged to indicate the current root node by signing a value associated with the node using an identity key associated with the key-handling unit.

47. Apparatus according to claim 35, wherein the key-handling unit is so arranged that only a particular type of key node, herein a dynamic key node, can be used as the current root node in addition to the node at the head of the hierarchy as judged without regard to which node is the current root node.

48. Apparatus according to claim 47, wherein the key-handling apparatus is arranged, upon receipt of a corresponding command, to generate a dynamic root node as a node of said key hierarchy.